



CS802E: E-cash

Name: Mayukh Datta

Roll no.: 16800116065

Reg. no.: 161680110032

Year: 4th

Dept: CSE



What is e-cash?

Ecash was conceived by David Chaum as an anonymous cryptographic electronic money or electronic cash system in 1983. It was realized through his corporation Digicash and used as micropayment system at one US bank from 1995 to 1998.



How it works?

Chaum published the idea of anonymous electronic money in a 1983 paper; eCash software on the user's local computer stored money in a digital format, cryptographically signed by a bank. The user could spend the digital money at any shop accepting eCash, without having to open an account with the vendor first, or transmitting credit card numbers. Security was ensured by public key digital signature schemes. The RSA blind signatures achieved unlinkability between withdrawal and spend transactions. Depending on the payment transactions, one distinguishes between on-line and off-line electronic cash: If the payee has to contact a third party (e.g., the bank or the credit-card company acting as an acquirer) before accepting a payment, the system is called an on-line system. In 1990, Chaum together with Moni Naor proposed the first off-line e-cash system, which was also based on blind signatures.



Properties

- Digital cash must have a monetary value; it must be backed by cash, bank-authorized credit, or a bank-certified cashier's check.
- When digital cash created by one bank is accepted by others, reconciliation must occur without any problems.
- Digital cash must be interoperable or exchangeable as payment for other digital cash, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfers, and the like.
- Digital cash must be storable and retrievable.
- Digital cash should not be easy to copy with while it is being exchanged.



Pros

- We can transfer funds, purchase stocks, and offer a variety of other services without having to handle physical cash or checks as long as bank is providing such services online.
- Debit cards and online bill payments allow immediate transfer of funds from an individual's personal account to a business's account regardless the designated place.
- Consumers will have greater privacy when shopping on the Internet using electronic money instead of ordinary credit cards.



Cons

- E-cash and E-Cash transaction security are the major concern.
- Frauds on E-Cash are on the catch recent years.
- Hackers with good skill able to hack into bank accounts and illegally retrieve of banking records has led to a widespread invasion of privacy and has promoted identity theft.



The End